Amendments to the Claims:

1. (Currently Amended) A method for securing transactions using electronic deposits (purses), comprising:

configuring, in an electronic deposit (purse), a grey lock mark being an attribute parameter of the electronic deposit (purse), which identifies the state of the last transaction of the electronic deposit (purse) as being one of complete and incomplete, the grey lock mark being configured to have one of a clear status when the last transaction was completed and a set (grey) status when the last transaction was incomplete, wherein[[;]] after setting the grey lock mark, all operations to the electronic deposit (purse) except resetting the grey lock mark being invalidated;

setting, while starting a transaction using the electronic deposit (purse), the grey lock mark and recording parameters of the transaction as a locking card source in the electronic deposit (purse); and

validating the recorded locking card source before debiting money from the electronic deposit (purse), and if the recorded parameters are validated, debiting money from the electronic deposit (purse) and resetting the grey lock mark simultaneously.

2. (Previously Presented) The method according to claim 1, further comprising:

storing an encryption key in a host computer of the distributor who distributes the electronic deposit (purse), in order to debit supplementary money from the electronic deposit (purse) and to reset the grey lock mark compulsorily in the electronic deposit (purse), which is being set the grey lock mark, on an on-line card terminal by an on-line mode.

3. (Previously Presented) The method according to claim 1, wherein the procedure of securing transactions using electronic deposits (purse) comprises:

inserting the electronic deposit (purse) into a transaction terminal;

authenticating mutually by the electronic deposit (purse) and the terminal;

setting the grey mark in the electronic deposit (purse) by the terminal;

performing a consumption; and

after the consumption is complete, debiting appropriate money from the electronic deposit (purse) resetting the grey mark simultaneously by the terminal.

4. (Previously Presented) The method according to claim 3, wherein the step of setting the grey lock mark comprises:

generating a first locking code by the electronic deposit (purse) according to the locking card source and transmitting simultaneously the locking card source to the transaction terminal using the electronic deposit (purse);

generating a second locking card code by the terminal in the same way as the electronic deposit (purse) and generating a first authentication code according to the second locking code and sending the first authentication code to the electronic deposit (purse);

generating a second authentication code by the electronic deposit (purse) according to the first locking code in the same was as the terminal;

determining whether the received first authentication code and the generated second authentication code are identical, and if yes, setting the grey lock mark; and

wherein the step of debiting money from the electronic deposit (purse) and resetting the grey lock mark simultaneously, comprises:

generating a third authentication code according to the second lock code and parameters for debiting money from the electronic deposit (purse) by the terminal, and sending the generated third authentication code and the parameters to the electronic deposit (purse);

generating a fourth authentication code according to the first lock code and the received parameters by the electronic deposit (purse); and

determining whether the received third authentication code and the generated fourth authentication code are identical, and if yes, debiting money from the electronic deposit (purse) and resetting the grey lock mark simultaneously after debiting successfully.

5. (Previously Presented) The method according to claim 4, wherein the step of validating the recorded locking card source comprises:

generating a fifth authentication code according to the first locking code by the electronic deposit (purse) and sending the fifth authentication code to the terminal;

generating a sixth authentication code according to the second locking code by the terminal and determining whether the received fifth authentication code and the generated sixth authentication code are identical, if yes, it means that the recorded locking card source is validated, otherwise, the recorded locking card source is invalidated; and

if the transaction using the electronic deposits (purses) is incomplete, the method further comprising:

storing the sixth authentication code and parameters for debiting money from the electronic deposits (purses) together as part of a grey record information by the terminal, and sending the grey record information to the host computer of the distributor who distributes the electronic deposit (purse); and

if the electronic deposit (purse) is used in any terminal that stores the grey record information, before validating the recorded locking card source, the method further comprising:

regenerating the fifth authentication code according to the recorded locking card source by the electronic deposit (purse) and send the fifth authentication code to the terminal.

6. (Previously Presented) The method according to claim 1, wherein the step of generating a first locking code according to the locking card source comprises:

generating a procedure encryption key (SESPK), correlating to at least a pseudo random number (ICC) created temporarily, in the electronic deposit (purse).

7. (Previously Presented) The method according to claim 6, wherein the equation of generating a procedure encryption key (SESPK) comprises:

the procedure encryption key (SESPK) = 3DES (DPK, DATA), where DPK is a consumption encryption key of the electronic deposit (purse); and DATA is a specific parameter including a pseudo random number (ICC) temporarily created by the electronic deposit (purse), a transaction sequence number of the electronic deposit (purse) (CTC), and the last two bytes of the terminal transaction sequence number (TTC).

8. (Previously Presented) The method according to claim 6, wherein the step of setting the grey lock mark comprises:

locking grey the IC card comprises:

sending a terminal transaction sequence number (TTC) to the electronic deposit (purse) by the terminal;

getting a pseudo random number (ICC) and an electronic deposit (purse) transaction sequence number (CTC) by the electronic deposit (purse);

generating a first procedure encryption key (SESPK) and recording the parameters of this generating step and also generating and recording a sixth authentication code of this time;

sending the pseudo random number (ICC) and the electronic deposit (purse) transaction sequence number (CTC) from the electronic deposit (purse) to the terminal, which has stored a consumption main encryption key (MPK) in its security authentication module (PSAM);

deriving the electronic deposit (purse) DPK by the security authentication module (PSAM); and

generating a second procedure encryption key (SESPK) by the terminal using the pseudo random number (ICC), the electronic deposit (purse) transaction sequence number (CTC), and the terminal transaction sequence number (TTC) in the same way as the electronic deposit (purse); and

wherein the step of debiting money from the electronic deposit (purse) and resetting the grey lock mark simultaneously comprises:

generating the third authentication code by the terminal according to the second procedure encryption key (SESPK), and at least the debit amount, operation date and time, and sending the third authentication code, the second procedure encryption key (SESPK), and at least the debit amount, operation date and time to the electronic deposit (purse);

generating the fourth authentication code by the electronic deposit (purse) according to the first procedure encryption key (SESPK), using the same data and algorithm as the terminal;

determining by the electronic deposit (purse) whether the third authentication code and the fourth authentication code are identical, and if yes, debiting money and resetting the grey lock mark, and otherwise, incrementing an internal error counter and returning an error code without debiting money from the electronic deposit (purse) and resetting the grey lock mark simultaneously; and

locking the electronic deposit (purse) internally to prevent misuse, when the internal error counter reaches a predetermined number.

9. (Previously Presented) The method according to claim 1, wherein the step of setting a grey lock mark comprises creating a refueling electronic deposit.

10. (Previously Presented) The method according to claim 9, wherein said refueling electronic deposit includes the functions of refueling transaction, local transaction for resetting the grey lock mark and on-line transaction for resetting the grey lock mark.

11. (Previously Presented) The method according to claim 9, wherein said refueling electronic deposit further includes the states of pre-refueling, grey lock and unlocked grey.

12. (Previously Presented) The method according to claim 9, wherein said refueling electronic deposit further comprises the commands of INITIALIZE FOR REFUEL, LOCK FOR REFUEL, DEBIT FOR REFUEL, INITIALIZE FOR UNLOCK, DEBIT FOR UNLOCK and GET GREY STATUS, wherein the INITIALIZE FOR REFUEL command is used for refueling consumption transaction initialization, the LOCK FOR REFUEL command is used for making grey lock to refueling electronic deposit (purse), the DEBIT FOR REFUEL command is used for local refueling consumption and unlocking grey simultaneously, the INITIALIZE FOR UNLOCK command is used for on-line unlocking and consumption transaction initialization, the DEBIT FOR UNLOCK command is used for on-line unlocking grey transaction and supplementary debiting refueling consumption simultaneously, and the GET GREY STATUS command is used for reading grey lock state and launching local unlocking grey transaction.